(3) It involves interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice; or

(4) It is determined with regard to the document, for good cause, that inviting the pubic comment is impracticable, unnecessary, or contrary to the public interest.

(c) *Procedures*—(1) *Normal case.* Unless the official having cognizance of a proposed regulatory document determines under the criteria of §701.66(b) that inviting public comment is not warranted, he or she shall cause it to be published in the FEDERAL REGISTER with an invitation for the public to submit comments in the form of written data, views, or arguments during a specified period of not less than 30 days following the date of publication. An opportunity for oral presentation normally will not be provided, but may be provided at the sole discretion of the official having cognizance of the proposed directive if he or she deems it to be in the best interest of the Department of the Navy or the public to do so. After careful consideration of all relevant matters presented within the period specified for public comment, the proposed document may be issued in final form. After issuance, the adopted document, and a preamble explaining the relationship of the adopted document to the proposed and the nature and effect of public comments, shall be published in the FEDERAL REGISTER for guidance of the public.

(2) *Where public comment is not warranted.* The official having cognizance of a proposed document within the purview of this paragraph shall, if he or she determines that inviting public comment concerning the document is not warranted under the criteria of §701.66(b), incorporate that determination, and the basis therefor, in the document when it is issued or submitted to a higher authority for issuance. After issuance, such document shall be published in the FEDERAL REGISTER for the guidance of the public, if required under §701.64(b).

§701.67 Petitions for issuance, revision, or cancellation of regulations affecting the public.

In accordance with the provisions of 32 CFR part 336, the Department of the Navy shall accord any interested person the right to petition in writing, for the issuance, revision, or cancellation of regulatory document that originates, or would originate, for the Department of the Navy, a policy, requirement, or procedure which is, or would be, within the purview of §701.66. The official having cognizance of the particular regulatory document involved, or having cognizance of the subject matter of a proposed document, shall give full and prompt consideration to any such petition. Such official may, at his or her absolute discretion, grant the petitioner an opportunity to appear, at his or her own expense, for the purpose of supporting the petition, if this is deemed to be compatible with orderly conduct of public business. The petitioner shall be advised in writing of the disposition, and the reasons for the disposition, of any petition within the purview of this section.

Subpart F—Department of the Navy Privacy Act Program

AUTHORITY: Pub. L. 93–579, 88 Stat 1896 (5 U.S.C. 552a).

SOURCE: 65 FR 31456, May 18, 2000, unless otherwise noted.

§701.100 Purpose.

Subparts F and G of this part implement the Privacy Act (5 U.S.C. 552a), and DoD Directive 5400.11,[1] and DoD 5400.11–R,[2] (32 CFR part 310) and provides Department of the Navy policies and procedures for:

(a) Governing the collection, safeguarding, maintenance, use, access, amendment, and dissemination of personal information kept by Department of the Navy in systems of records;

[1] Copies may be obtained: http://www.whs.osd.mil/corres.htm.

[2] See footnote 1 to §701.100.

(b) Notifying individuals if any systems of records contain a record pertaining to them;

(c) Verifying the identity of individuals who request their records before the records are made available to them;

(d) Notifying the public of the existence and character of each system of records.

(e) Exempting systems of records from certain requirements of the Privacy Act; and

(f) Governing the Privacy Act rules of conduct for Department of the Navy personnel, who will be subject to criminal penalties for noncompliance with 5 U.S.C. 552a, as amended by the Computer Matching Act of 1988.

§ 701.101 Applicability.

This subpart and subpart G of this part apply throughout the Department of the Navy. It is also applicable to contractors by contract or other legally binding action, whenever a Department of the Navy contract provides for the operation of a system of records or portion of a system of records to accomplish a Department of the Navy function. For the purposes of any criminal liabilities adjudged, any contractor or any employee of such contractor is considered to be an employee of Department of the Navy. In case of a conflict, this subpart and subpart G of this part take precedence over any existing Department of the Navy directive that deals with the personal privacy and rights of individuals regarding their personal records, except for disclosure of personal information required by 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act and implemented by Secretary of the Navy Instruction 5720.42F,[3] 'Department of the Navy Freedom of Information Act Program.'

§ 701.102 Definitions.

For the purposes of this subpart and subpart G of this part, the following meanings apply.

Access. The review or copying of a record or parts thereof contained in a system of records by any individual.

Agency. For the purposes of disclosing records subject to the Privacy Act between or among Department of Defense (DoD) components, the Department of Defense is considered a single agency. For all other purposes, Department of the Navy is considered an agency within the meaning of Privacy Act.

Confidential source. A person or organization who has furnished information to the Federal Government either under an express promise that the person's or the organization's identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

Defense Data Integrity Board. Consists of members of the Defense Privacy Board, as outlined in DoD Directive 5400.11 and, in addition, the DoD Inspector General or the designee, when convened to oversee, coordinate and approve or disapprove all DoD component computer matching covered by the Privacy Act.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review), to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

Federal personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals or survivors thereof, entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

Individual. A living citizen of the United States or alien lawfully admitted to the U.S. for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a deceased person under this instruction and the term ''individual'' does not embrace an individual

[3] Copies may be obtained: Chief of Naval Operations, 2000 Navy Pentagon, Washington, DC 20350–2000.

acting in a non-personal capacity (for example, sole proprietorship or partnership).

Individual access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Maintain. Includes maintain, collect, use, or disseminate.

Member of the public. Any individual or party acting in a private capacity.

Minor. Under this subpart and subpart G of this part, a minor is an individual under 18 years of age, who is not a member of the U.S. Navy or Marine Corps, nor married.

Official use. Under this subpart and subpart G of this part, this term is used when Department of the Navy officials and employees have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties.

Personal information. Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

Privacy Act (PA) request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Record. Any item, collection, or grouping of information about an individual that is maintained by a naval activity including, but not limited to, the individual's education, financial transactions, and medical, criminal, or employment history, and that contains the individual's name or other identifying particulars assigned to the individual, such as a finger or voice print or a photograph.

Review authority. An official charged with the responsibility to rule on administrative appeals of initial denials of requests for notification, access, or amendment of records. The Secretary of the Navy has delegated his review authority to the Assistant Secretary of the Navy (Manpower and Reserve Affairs (ASN(MRA)), the General Counsel (OGC), and the Judge Advocate General (NJAG). Additionally, the Office of Personnel Management (OPM) is the review authority for civilian official personnel folders or records contained in any other OPM record.

Risk assessment. An analysis which considers information sensitivity, vulnerability, and cost to a computer facility or word processing center in safeguarding personal information processed or stored in the facility or center.

Routine use. Disclosure of a record outside the Department of Defense for a purpose that is compatible with the purpose for which the record was collected and maintained by the Department of Defense. The routine use must have been included in the notice for the system of records published in the FEDERAL REGISTER.

Statistical record. A record maintained only for statistical research, or reporting purposes, and not used in whole or in part in making any determination about a specific individual.

System manager. An official who has overall responsibility for a system of records. He or she may serve at any level in Department of the Navy. Systems managers are indicated in the published record systems notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records, at the local activity).

System of records. A group of records under the control of a Department of the Navy activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all Privacy Act systems of records must be published in the FEDERAL REGISTER and are also published in periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211.[4]

Word processing equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programmable software, hard wiring, or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to receive information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device.

[4] See footnote 3 to § 701.101.

Word processing system. A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written communications into a form suitable to the originator. The results are written or graphic presentations intended to communicate verbally or visually with another individual.

Working day. All days excluding Saturday, Sunday, and legal holidays.

§ 701.103 Policy.

It is the policy of Department of the Navy to:

(a) Ensure that all its personnel comply fully with 5 U.S.C. 552a, DoD Directive 5400.11 and DoD 5400.11–R, to protect individuals from unwarranted invasions of privacy. Individuals covered by this protection are living citizens of the U.S. or aliens lawfully admitted for permanent residence. A legal guardian of an individual or parent of a minor when acting on the individual's or minor's behalf, has the same rights as the individual or minor. (A member of the Armed Forces is not a minor for the purposes of this subpart and subpart G of this part).

(b) Collect, maintain, and use only that personal information needed to support a Navy function or program as authorized by law or E.O., and disclose this information only as authorized by 5 U.S.C. 552a and this subpart and subpart G of this part. In assessing need, consideration shall be given to alternatives, such as use of information not individually identifiable or use of sampling of certain data for certain individuals only. Additionally, consideration is to be given to the length of time information is needed, and the cost of maintaining the information compared to the risks and adverse consequences of not maintaining the information.

(c) Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(d) Let individuals have access to, and obtain copies of, all or portions of their records, subject to exemption procedures authorized by law and this subpart and subpart G of this part.

(e) Let individuals request amendment of their records when discrepancies proven to be erroneous, untimely, incomplete, or irrelevant are noted.

(f) Let individuals request an administrative review of decisions that deny them access, or refuse to amend their records.

(g) Ensure that adequate safeguards are enforced to prevent misuse, unauthorized disclosure, alteration, or destruction of personal information in records.

(h) Maintain no records describing how an individual exercises his or her rights guaranteed by the First Amendment (freedom of religion, political beliefs, speech, and press; peaceful assemblage; and petition for redress of grievances), unless they are:

(1) Expressly authorized by statute;

(2) Authorized by the individual;

(3) Within the scope of an authorized law enforcement activity; or

(4) For the maintenance of certain items of information relating to religious affiliation for members of the naval service who are chaplains. This should not be construed, however, as restricting or excluding solicitation of information which the individual is willing to have in his or her record concerning religious preference, particularly that required in emergency situations.

(5) Maintain only systems of records which have been published in the FEDERAL REGISTER, in accordance with periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211 and § 701.105. These OPNAVNOTEs 5211 provide a listing of all Department of the Navy Privacy Act systems of records and identify the Office of Personnel Management (OPM) government-wide systems containing information on Department of the Navy civilian employees, even though technically, Department of the Navy does not have cognizance over them. A Privacy Act systems notice outlines what kinds of information may be collected and maintained by naval activities. When collecting/maintaining information in a Privacy Act system of records, review the systems notice to ensure activity compliance is within the scope of the system. If you determine the systems

notice does not meet your needs, contact the systems manager or Chief of Naval Operations (N09B30) with your concerns so that amendment of the system may be considered.

§ 701.104 Responsibility and authority.

(a) *Chief of Naval Operations (CNO).* CNO is designated as the official responsible for administering and supervising the execution of 5 U.S.C. 552a, DoD Directive 5400.11, and DoD 5400.11–R. CNO has designated the Assistant Vice Chief of Naval Operations (N09B30) as principal Privacy Act Coordinator for the Department of the Navy to:

(1) Set Department of the Navy policy on the provisions of the Privacy Act.

(2) Serve as principal advisor on all Privacy Act matters.

(3) Oversee the administration of the Privacy Act program, which includes preparing the Department of the Navy Privacy Act report for submission to Congress.

(4) Develop Navy-wide Privacy Act training program and serve as training-oversight manager.

(5) Conduct staff assistance visits within Department of the Navy to review compliance with 5 U.S.C. 552a and this subpart and subpart G of this part.

(6) Coordinate and prepare responses for Privacy Act requests received for Office of the Secretary of the Navy records.

(b) *Commandant of the Marine Corps (CMC).* CMC is responsible for administering and supervising the execution of this subpart and subpart G of this part within the Marine Corps. The Commandant has designated the Director, Manpower Management Information Systems Division (HQMC (Code ARAD)) as the Privacy Act coordinator for Headquarters, U.S. Marine Corps.

(c) *Privacy Act Coordinator.* Each addressee is responsible for implementing and administering a Privacy Act program under this subpart and subpart G of this part. Each addressee shall designate a Privacy Act Coordinator to:

(1) Serve as principal point of contact on Privacy Act matters.

(2) Provide training for activity/command personnel on the provisions of 5 U.S.C. 552a and this subpart and subpart G of this part.

(3) Issue implementing instruction which designates the activity's Privacy Act Coordinator, Privacy Act records disposition, Privacy Act processing procedures, identification of Privacy Act systems of records under their cognizance, and training aids for those personnel involved with systems of records.

(4) Review internal directives, practices, and procedures, including those having Privacy Act implications and where Privacy Act Statements (PASs) are needed.

(5) Compile input and submit consolidated Privacy Act report to Echelon 2 Privacy Act Coordinator, who, in turn, will provide consolidated report to CNO (N09B30).

(6) Maintain liaison with records management officials (i.e., maintenance and disposal procedures and standards, forms, and reports), as appropriate.

(7) Provide guidance on handling Privacy Act requests and scope of Privacy Act exemptions.

(8) Conduct staff assistance visits within command and lower echelon commands to ensure compliance with the Privacy Act.

(9) Echelon 2 Privacy Act Coordinators shall provide CNO (N09B30) with a complete listing of all Privacy Act Coordinators under their jurisdiction. Such information should include activity name and address, office code, name of Privacy Act Coordinator, commercial and DSN telephone number, and FAX number, if applicable.

(d) *Release authority.* Officials having cognizance over the requested subject matter are authorized to respond to requests for notification, access, and/or amendment of records. These officials could also be systems managers (see § 701.104(g)).

(e) *Denial authority.* Within the Department of the Navy, the following chief officials, their respective vice commanders, deputies, principal assistants, and those officials specifically designated by the chief official are authorized to deny requests, either in whole or in part, for notification, access and amendment, made under this subpart and subpart G of this part, when the records relate to matters

within their respective areas of responsibility or chain of command:

(1) Department of the Navy. Civilian Executive Assistants; CNO; CMC; Chief of Naval Personnel; Commanders of the Naval Systems Commands, Office of Naval Intelligence, Naval Security Group Command, Naval Imaging Command, and Naval Computer and Telecommunications Command; Chief, Bureau of Medicine and Surgery; Auditor General of the Navy; Naval Inspector General; Director, Office of Civilian Personnel Management; Chief of Naval Education and Training; Commander, Naval Reserve Force; Chief of Naval Research; Commander, Naval Oceanography Command; heads of Department of the Navy Staff Offices, Boards, and Councils; Flag Officers and General Officers. NJAG and his Deputy, and OGC and his Deputies are excluded from this grant of authorization. While NJAG and OGC are not denial authorities, they are authorized to further delegate the authority conferred here to other senior officers/officials within NJAG and OGC.

(2) For the shore establishment.(i) All officers authorized under Article 22, Uniform Code of Military Justice (UCMJ) or designated in section 0120, Manual of the Judge Advocate General (JAGINST 5800.7C),[5] to convene general courts-martial.

(ii) Commander, Naval Investigative Service Command.

(iii) Deputy Commander, Naval Legal Service Command.

(3) In the Operating Forces. All officers authorized by Article 22, Uniform Code of Military Justice (UCMJ), or designated in section 0120, Manual of the Judge Advocate General (JAGINST 5800.7C), to convene general courts-martial.

(f) *Review authority*. (1) The Assistant Secretary of the Navy (Manpower and Reserve Affairs), is the Secretary's designee, and shall act upon requests for administrative review of initial denials of requests for amendment of records related to fitness reports and performance evaluations of military personnel (see § 701.111(c)(3)).

(2) The Judge Advocate General and General Counsel, as the Secretary's designees, shall act upon requests for administrative review of initial denials of records for notification, access, or amendment of records, as set forth in § 701.111(c)(2) and (4).

(3) The authority of the Secretary of the Navy (SECNAV), as the head of an agency, to request records subject to the Privacy Act from an agency external to the Department of Defense for civil or criminal law enforcement purposes, under subsection (b)(7) of 5 U.S.C. 552a, is delegated to the Commandant of the Marine Corps, the Director of Naval Intelligence, the Judge Advocate General, and the General Counsel.

(g) *Systems manager*. Systems managers, as designated in Department of the Navy's compilation of systems notices (periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211,[6] ''Current Privacy Act Issuances'') shall:

(1) Ensure the system has been published in the FEDERAL REGISTER and that any additions or significant changes are submitted to CNO (N09B30) for approval and publication. The systems of records should be maintained in accordance with the systems notices as published in the periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances.''

(2) Maintain accountability records of disclosures.

(h) *Department of the Navy employees.* Each employee of the Department of the Navy has certain responsibilities for safeguarding the rights of others. These include:

(1) Not disclosing any information contained in a system of records by any means of communication to any person or agency, except as authorized by this subpart and subpart G of this part.

(2) Not maintaining unpublished official files which would fall under the provisions of 5 U.S.C. 552a.

(3) Safeguarding the privacy of individuals and confidentiality of personal

[5] Copies may be obtained: Judge Advocate General, Navy Department, 1322 Patterson Avenue, SE, Suite 3000, Washington Navy Yard, Washington, DC 20374-5066.

[6] See footnote 3 to § 701.101.

information contained in a system of records.

§ 701.105 Systems of records.

To be subject to this subpart and subpart G of this part, a ''system of records'' must consist of ''records'' that are retrieved by the name, or some other personal identifier, of an individual and be under the control of Department of the Navy.

(a) *Retrieval practices.* (1) Records in a group of records that are not retrieved by personal identifiers are not covered by this subpart and subpart G of this part, even if the records contain information about individuals and are under the control of Department of the Navy. The records must be retrieved by personal identifiers to become a system of records.

(2) If records previously not retrieved by personal identifiers are rearranged so they are retrieved by personal identifiers, a new system notice must be submitted in accordance with § 701.107.

(3) If records in a system of records are rearranged so retrieval is no longer by personal identifiers, the records are no longer subject to this subpart and subpart G of this part and the records system notice should be deleted in accordance with § 701.107.

(b) *Recordkeeping standards.* A record maintained in a system of records subject to this subpart and subpart G of this part must meet the following criteria:

(1) Be accurate. All information in the record must be factually correct.

(2) Be relevant. All information contained in the record must be related to the individual who is the record subject and also must be related to a lawful purpose or mission of the Department of the Navy activity maintaining the record.

(3) Be timely. All information in the record must be reviewed periodically to ensure that it has not changed due to time or later events.

(4) Be complete. It must be able to stand alone in accomplishing the purpose for which it is maintained.

(5) Be necessary. All information in the record must be needed to accomplish a Department of the Navy mission or purpose established by Federal Law or E.O. of the President.

(c) *Authority to establish systems of records.* Identify the specific Federal statute or E.O. of the President that authorizes maintaining each system of records. When a naval activity uses its ''internal housekeeping'' statute, i.e., 5 U.S.C. 301, Departmental Regulations, the naval instruction that implements the statute should also be identified. A statute or E.O. authorizing a system of records does not negate the responsibility to ensure the information in the system of records is relevant and necessary.

(d) *Exercise of First Amendment rights.* (1) Do not maintain any records describing how an individual exercises rights guaranteed by the First Amendment of the U.S. Constitution unless expressly authorized by Federal law; the individual; or pertinent to and within the scope of an authorized law enforcement activity.

(2) First amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

(e) *System manager's evaluations and reviews.* (1) Evaluate each new system of records. Before establishing a system of records, evaluate the information to be included and consider the following:

(i) The relationship of each item of information to be collected and retained to the purpose for which the system is maintained (all information must be relevant to the purpose);

(ii) The specific impact on the purpose or mission if each category of information is not collected (all information must be necessary to accomplish a lawful purpose or mission.);

(iii) The ability to meet the informational needs without using personal identifiers (will anonymous statistical records meet the needs?);

(iv) The length of time each item of information must be kept;

(v) The methods of disposal;

(vi) The cost of maintaining the information; and

(vii) Whether a system already exists that serves the purpose of the new system.

(2) Evaluate and review all existing systems of records.

(i) When an alteration or amendment of an existing system is prepared pursuant to § 701.107(b) and (c), do the evaluation described in paragraph (e) of this section.

(ii) Conduct the following reviews annually and be prepared to report, in accordance with § 701.104(c)(8), the results and corrective actions taken to resolve problems uncovered.

(A) Training practices to ensure all personnel are familiar with the requirements of 5 U.S.C. 552a, and DoD Directive 5400.11, ''DoD Privacy Program'', this subpart and subpart G of this part, and any special needs their specific jobs entail.

(B) Recordkeeping and disposal practices to ensure compliance with this subpart and subpart G of this part.

(C) Ongoing computer matching programs in which records from the system have been matched with non-DoD records to ensure that the requirements of § 701.115 have been met.

(D) Actions of Department of the Navy personnel that resulted in either Department of the Navy being found civilly liable or a person being found criminally liable under 5 U.S.C. 552a, to determine the extent of the problem and find the most effective way of preventing the problem from occurring in the future.

(E) Each system of records notice to ensure it accurately describes the system. Where major changes are needed, alter the system notice in accordance with § 701.107(b). If minor changes are needed, amend the system notice pursuant to § 701.107(c).

(iii) Every even-numbered year, review a random sample of Department of the Navy contracts that provide for the operation of a system of records to accomplish a Department of the Navy function, to ensure the wording of each contract complies with the provisions of 5 U.S.C. 552a and paragraph (h) of this section.

(iv) Every three years, beginning in 1992, review the routine use disclosures associated with each system of records to ensure the recipient's use of the records continues to be compatible with the purpose for which the information was originally collected.

(v) Every three years, beginning in 1993, review each system of records for which exemption rules have been established to determine whether each exemption is still needed.

(vi) When directed, send the reports through proper channels to the CNO (N09B30).

(f) *Discontinued information requirements.* (1) Immediately stop collecting any category or item of information about individuals that is no longer justified, and when feasible, remove the information from existing records.

(2) Do not destroy records that must be kept in accordance with retention and disposal requirements established under SECNAVINST 5212.5,[7] ''Disposal of Navy and Marine Corps Records.''

(g) *Review records before disclosing outside the Federal government.* Before disclosing a record from a system of records to anyone outside the Federal government, take reasonable steps to ensure the record which is being disclosed is accurate, relevant, timely, and complete for the purposes it is being maintained.

(h) *Federal government contractors*—(1) *Applicability to Federal government contractors.* (i) When a naval activity contracts for the operation of a system of records to accomplish its function, the activity must ensure compliance with this subpart and subpart G of this part and 5 U.S.C. 552a. For the purposes of the criminal penalties described in 5 U.S.C. 552a, the contractor and its employees shall be considered employees of the agency during the performance of the contract.

(ii) Consistent with parts 24 and 52 of the Federal Acquisition Regulation (FAR), contracts for the operation of a system of records shall identify specifically the record system and the work to be performed, and shall include in the solicitations and resulting contract the terms as prescribed by the FAR.

(iii) If the contractor must use records that are subject to this subpart and subpart G of this part to perform any part of a contract, the contractor activities are subject to this subpart and subpart G of this part.

[7] Copies may be obtained: OPNAV/SECNAV Directives Control Office, Washington Navy Yard, Building 200, Washington, DC 20350–2000.

(iv) This subpart and subpart G of this part do not apply to records of a contractor that are:

(A) Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

(B) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the naval activity;

(C) Maintained as training records by an educational organization contracted by a naval activity to provide training when the records of the contract students are similar to and commingled with training records of other students, such as admission forms, transcripts, and academic counseling and similar records; or

(D) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with 31 U.S.C. 952d.

(v) For contracting that is subject to this subpart and subpart G of this part, naval activities shall publish instructions that:

(A) Furnish Privacy Act guidance to personnel who solicit, award, or administer Government contracts;

(B) Inform prospective contractors of their responsibilities under this subpart and subpart G of this part and the Department of the Navy Privacy Program;

(C) Establish an internal system for reviewing contractor's performance for compliance with the Privacy Act; and

(D) Provide for the biennial review of a random sample of contracts that are subject to this subpart and subpart G of this part.

(2) *Contracting procedures.* The Defense Acquisition Regulatory (DAR) Council, which oversees the implementation of the FAR within the Department of Defense, is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts that are subject to this subpart and subpart G of this part and 5 U.S.C. 552a.

(3) *Contractor compliance.* Naval activities shall establish contract surveillance programs to ensure contractors comply with the procedures established by the DAR Council under the preceding subparagraph.

(4) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a contract let by a naval activity is considered a disclosure within Department of the Navy. The contractor is considered the agent of Department of the Navy when receiving and maintaining the records for that activity.

§ 701.106 Safeguarding records in systems of records.

Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(a) *Minimum standards.* (1) Conduct risk analysis and management planning for each system of records. Consider sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards. The risk analysis may vary from an informal review of a small, relatively insensitive system to a formal, fully quantified risk analysis of a large, complex, and highly sensitive system.

(2) Train all personnel operating a system of records or using records from a system of records in proper record security procedures.

(3) Label information exempt from disclosure under this subpart and subpart G of this part to reflect their sensitivity, such as ''FOR OFFICIAL USE ONLY,'' ''PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW BASIS ONLY,'' or some other statement that alerts individuals of the sensitivity to the records.

(4) Administer special administrative, physical, and technical safeguards to protect records processed or stored in an automated data processing or word processing system to protect them from threats unique to those environments.

(b) *Records disposal.* (1) Dispose of records from systems of records so as

to prevent inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (*i.e.*, such as tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) The transfer of large volumes of records (*e.g.*, printouts and computer cards) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records, if the volume of records, coding of the information, or some other factor render it impossible to recognize any personal information about a specific individual.

(3) When disposing or destroying large quantities of records from a system of records, care must be taken to ensure that the bulk of the records is maintained to prevent easy identification of specific records. If such bulk is maintained, no special procedures are required. If bulk is not maintained, or if the form of the records makes individually identifiable information easily discernable, dispose of the records in accordance with paragraph (b)(1) of this section.

§ 701.107 Criteria for creating, altering, amending and deleting Privacy Act systems of records.

(a) *Criteria for a new system of records.* A new system of records is one for which no existing system notice has been published in the FEDERAL REGISTER. If a notice for a system of records has been canceled or deleted, and it is determined that it should be reinstated or reused, a new system notice must be published in the FEDERAL REGISTER. Advance public notice must be given before a naval activity may begin to collect information for or use a new system of records. The following procedures apply:

(1) Describe in the record system notice the contents of the record system and the purposes and routine uses for which the information will be used and disclosed.

(2) The public shall be given 30 days to comment on any proposed routine uses before the routine uses are implemented.

(3) The notice shall contain the date the system of records will become effective.

(b) *Criteria for an alteration to a system of records notice.* A system is considered altered when any one of the following actions occur or is proposed:

(1) A significant increase or change in the number or types of individuals about whom records are maintained. For example, a decision to expand a system of records that originally covered personnel assigned to only one naval activity to cover personnel at several installations would constitute an altered system. An increase or decrease in the number of individuals covered due to normal growth or decrease is not an alteration.

(2) A change that expands the types or categories of information maintained. For example, a personnel file that has been expanded to include medical records would be an alteration.

(3) A change that alters the purpose for which the information is used. In order to be an alteration, the change must be one that is not reasonably inferred from any of the existing purposes.

(4) A change to equipment configuration (either hardware or software) that creates substantially greater use of records in the system. For example, placing interactive computer terminals at regional offices when the system was formerly used only at the headquarters would be an alteration.

(5) A change in the manner in which records are organized or in the method by which records are retrieved.

(6) Combining record systems due to a reorganization within Department of the Navy.

(7) Retrieving by Social Security Numbers (SSNs), records that previously were retrieved only by names would be an alteration if the present notice failed to indicate retrieval by SSNs. An altered system of records must be published in the FEDERAL REGISTER. Submission for an alteration must contain a narrative statement, the specific changes altering the system, and the system of records notice.

(c) *Criteria for amending a systems of records notice.* Minor changes to published system of records notices are considered amendments. All amendments should be forwarded to CNO (N09B30) for publication in the FEDERAL REGISTER. When submitting an amendment to a system of records notice, the naval activity must include a description of the specific changes proposed and the system of records notice.

(d) *Criteria for deleting a system of records notice.* When a system of records is discontinued, incorporated into another system, or determined to be no longer subject to this subpart and subpart G of this part, a deletion notice must be published in the FEDERAL REGISTER. The deletion notice shall include the system identification number, system name, and the reason for deleting it. If a system is deleted through incorporation into or merger with another system, identify the successor system in the deletion notice.

§ 701.108 Collecting information about individuals.

(a) *Collecting directly from the individual.* To the greatest extent practicable, collect information for systems of records directly from the individual to whom the record pertains if the record may be used to make an adverse determination about the individual's rights, benefits, or privileges under the Federal programs.

(b) *Collecting information about individuals from third persons.* It might not always be practical to collect all information about an individual directly from that person, such as verifying information through other sources for security or employment suitability determinations; seeking other opinions, such as a supervisor's comments on past performance or other evaluations; obtaining the necessary information directly from the individual would be exceptionally difficult or would result in unreasonable costs or delays; or, the individual requests or consents to contacting another person to obtain the information.

(c) *Soliciting the social security number (SSN).* (1) It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, this prohibition does not apply if a Federal law requires that the SSN be provided, or the SSN is required by a law or regulation adopted before January 1, 1975, to verify the individual's identity for a system of records established and in use before that date.

(2) Before requesting an individual to provide the SSN, the individual must be advised whether providing the SSN is mandatory or voluntary; by what law or other authority the SSN is solicited; and what uses will be made of the SSN.

(3) The preceding advice relates only to the SSN. If other information about the individual is solicited for a system of records, a Privacy Act statement (PAS) also must be provided to him/her.

(4) The notice published in the FEDERAL REGISTER for each system of records containing SSNs solicited from individuals must indicate the authority for soliciting the SSNs and whether it is mandatory for the individuals to provide their SSNs. E.O. 9397 requires federal agencies to use SSNs as numerical identifiers for individuals in most federal records systems, however, it does not make it mandatory for individuals to provide their SSNs.

(5) When entering military service or civilian employment with the Department of the Navy, individuals must provide their SSNs. This is then the individual's numerical identifier and is used to establish personnel, financial, medical, and other official records (as authorized by E.O. 9397). The individuals must be given the notification described above. Once the individual has provided his or her SSN to establish the records, a notification is not required when the SSN is requested only for identification or to locate the records.

(6) The Federal Personnel Manual[8] must be consulted when soliciting SSNs for use in systems of records maintained by the Office of Personnel Management.

[8] Copies may be obtained: Office of Personnel Management, 1900 E Street, Washington, DC 20415.

(7) A Department of the Navy activity may request an individual's SSN even though it is not required by Federal statute, or is not for a system of records in existence and operating prior to January 1, 1975. However, the separate Privacy Act Statement for the SSN, alone, or a merged Privacy Act Statement covering both the SSN and other items of personal information, must make clear that disclosure of the number is voluntary. If the individual refuses to disclose his or her SSN, the activity must be prepared to identify the individual by alternate means.

(d) *Contents of Privacy Act Statement.* (1) When an individual is requested to furnish information about himself/herself for a system of records, a Privacy Act Statement must be provided to the individual, regardless of the method used to collect the information (*i.e.,* forms, personal or telephonic interview, etc). If the information requested will not be included in a system of records, a Privacy Act Statement is not required.

(2) The Privacy Act Statement shall include the following:

(i) The Federal law or E.O. that authorizes collecting the information (*i.e.,* E.O. 9397 authorizes collection of SSNs);

(ii) Whether or not it is mandatory for the individual to provide the requested information (It is only mandatory when a Federal law or E.O. of the President specifically imposes a requirement to furnish the information and provides a penalty for failure to do so. If furnishing information is a condition for granting a benefit or privilege voluntarily sought by the individual, it is voluntary for the individual to give the information.);

(iii) The principle purposes for collecting the information;

(iv) The routine uses that will be made of the information (*i.e.,* to whom and why it will be disclosed outside the Department of Defense); and

(v) The possible effects on the individual if the requested information is not provided.

(3) The Privacy Act Statement must appear on the form used to collect the information or on a separate form that can be retained by the individual collecting the information. If the information is collected by means other than a form completed by the individual, *i.e.,* solicited over the telephone, the Privacy Act Statement should be read to the individual and if requested by the individual, a copy sent to him/her. There is no requirement that the individual sign the Privacy Act Statement.

(e) *Format for Privacy Act Statement.* When forms are used to collect information about individuals for a system of records, the Privacy Act Statement shall appear as follows (listed in the order of preference):

(1) Immediately below the title of the form,

(2) Elsewhere on the front page of the form (clearly indicating it is the Privacy Act Statement),

(3) On the back of the form with a notation of its location below the title of the form, or

(4) On a separate form which the individual may keep.

§ 701.109 Access to records.

(a) *Individual access to records.* (1) *Right of access.* Only individuals who are subjects of records maintained in systems of records and by whose personal identifiers the records are retrieved have the right of individual access under this subpart and subpart G of this part, unless they provide written authorization for their representative to act on their behalf. Legal guardians or parents acting on behalf of a minor child also have the right of individual access under this subpart and subpart G of this part.

(2) *Notification of record's existence.* Each naval activity shall establish procedures for notifying an individual, in response to his or her request, if a system of records identified by him/her contains a record pertaining to the individual.

(3) *Individual request for access.* Individuals shall address requests for access to records in systems of records to the system manager or the office designated in the Department of the Navy compilation of system notices (periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances'').

(4) *Verifying identity.* (i) An individual shall provide reasonable verification of

identity before obtaining access to records.

(ii) When requesting records in writing, naval activities may not insist that a requester submit a notarized signature. The courts have ruled that an alternative method of verifying identity must be established for individuals who do not have access to notary services. This alternative permits requesters to provide an unsworn declaration that states ''I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct.''

(iii) When an individual seeks access in person, identification can be verified by documents normally carried by the individual (*i.e.*, identification card, driver's license, or other license, permit or pass normally used for identification purposes).

(iv) When access is requested other than in writing, identity may be verified by the individual's providing minimum identifying data such as full name, date and place of birth, or other information necessary to locate the record sought. If the information sought is sensitive, additional identifying data may be required. Telephonic requests should not be honored.

(v) Allow an individual to be accompanied by a person of his or her choice when viewing the record; however, require the individual to provide written authorization to have the record discussed in front of the other person.

(vi) Do not deny access to an individual who is the subject of the record solely for refusing to divulge his or her SSN, unless it is the only means of retrieving the record or verifying identity.

(vii) Do not require the individual to explain why he or she is seeking access to a record under this subpart and subpart G of this part.

(viii) Only a designated denial authority may deny access. The denial must be in writing and contain the information required by paragraph (d) of this section.

(5) *Blanket requests not honored.* Do not honor requests from individuals for notification and/or access concerning all Department of the Navy systems of records. In these instances, notify the individual that requests for notification and/or access must be directed to the appropriate system manager for the particular record system being requested, as indicated in the periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances''; and the request must either designate the particular system of records to be searched, or provide sufficient information for the system manager to identify the appropriate system. Also, provide the individual with any other information needed for obtaining consideration of his or her request.

(6) *Granting individual access to records.* (i) Grant the individual access to the original record (or exact copy) without any changes or deletions, other than those made in accordance with § 701.113.

(ii) Grant the individual's request for an exact copy of the record, upon the signed authorization of the individual, and provide a copy to anyone designated by the individual. In either case, the copying fees may be assessed to the individual pursuant to § 701.109(b).

(iii) If requested, explain any record or portion of a record that is not understood, as well as any changes or deletions.

(7) *Illegible or incomplete records.* Do not deny an individual access solely because the physical condition or format of the record does not make it readily available (*i.e.*, when the record is in a deteriorated state or on magnetic tape). Either prepare an extract or recopy the document exactly.

(8) *Access by parents and legal guardians.* (i) The parent of any minor, or the legal guardian of any individual declared by a court of competent jurisdiction to be incompetent due to physical or mental incapacity or age, may obtain access to the record of the minor or incompetent individual if the parent or legal guardian is acting on behalf or for the benefit of the minor or incompetent. However, with respect to access by parents and legal guardians to medical records and medical determinations about minors, use the following procedures:

(A) In the United States, the laws of the state where the records are located

might afford special protection to certain medical records (*i.e.*, drug and alcohol abuse treatment, and psychiatric records). The state statutes might apply even if the records are maintained by a naval medical facility.

(B) For installations located outside the U.S., the parent or legal guardian of a minor shall be denied access if all four of the following conditions are met:

(1) The minor at the time of the treatment or consultation was 15, 16, or 17 years old;

(2) The treatment or consultation was within a program authorized by law or regulation to provide confidentiality to the minor;

(3) The minor indicated a desire that the treatment or consultation record be handled in confidence and not disclosed to a parent or guardian; and

(4) The parent or legal guardian does not have the written authorization of the minor or a valid court order granting access.

(ii) A minor or incompetent has the same right of access as any other individual under this subpart and subpart G of this part. The right of access of the parent or legal guardian is in addition to that of the minor or incompetent.

(9) *Access to information compiled in reasonable anticipation of a civil proceeding.* (i) An individual is not entitled under this subpart and subpart G of this part to access information compiled in reasonable anticipation of a civil action or proceeding.

(ii) The term ''civil action or proceeding'' includes quasi-judicial and pre-trial judicial proceedings, as well as formal litigation.

(iii) Paragraphs (a)(9)(i) and (ii) of this section do not prohibit access to records compiled or used for purposes other than litigation, nor prohibit access to systems of records solely because they are frequently subject to litigation. The information must have been compiled for the primary purpose of litigation.

(10) *Personal notes or records not under the control of the Department of the Navy.* (i) Certain documents under the control of a Department of the Navy employee and used to assist him/her in performing official functions are not considered Department of the Navy records within the meaning of this subpart and subpart G of this part. These documents are not systems of records that are subject to this subpart and subpart G of this part, if they are:

(A) Maintained and discarded solely at the discretion of the author;

(B) Created only for the author's personal convenience;

(C) Not the result of official direction or encouragement, whether oral or written; and

(D) Not shown to other persons for any reason or filed in agency files.

(ii) [Reserved]

(11) *Relationship between the Privacy Act and FOIA.* In some instances, individuals requesting access to records pertaining to themselves may not know which Act to cite as the appropriate statutory authority. The following guidelines are to ensure that the individuals receive the greatest degree of access under both Acts:

(i) Access requests that specifically state or reasonably imply that they are made under 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act of 1986, are processed under Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program.''

(ii) Access requests that specifically state or reasonably imply that they are made under 5 U.S.C. 552a are processed under this subpart and subpart G of this part.

(iii) Access requests that cite both 5 U.S.C. 552a, as amended by the Computer Matching Act of 1988 and 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act are processed under the Act that provides the greater degree of access. Inform the requester which instruction was used in granting or denying access.

(iv) Do not penalize the individual access to his or her records otherwise releasable under 5 U.S.C. 552a and periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances'', simply because he or she failed to cite the appropriate statute or instruction.

(12) *Time limits.* Acknowledge requests for access made under Privacy Act or this subpart and subpart G of this part within 10 working days after receipt,

and advise the requester of your decision to grant/deny access within 30 working days.

(b) *Reproduction fees.* Normally, only one copy of any record or document will be provided. Checks or money orders for fees should be made payable to the Treasurer of the United States and deposited to the miscellaneous receipts of the treasury account maintained at the finance office servicing the activity.

(1) Fee schedules shall include only the direct cost of reproduction and shall not include costs of:

(i) Time or effort devoted to searching for or reviewing the record by naval personnel;

(ii) Fees not associated with the actual cost of reproduction;

(iii) Producing a copy when it must be provided to the individual without cost under another regulation, directive, or law;

(iv) Normal postage;

(v) Transportation of records or personnel; or

(vi) Producing a copy when the individual has requested only to review the record and has not requested a copy to keep, and the only means of allowing review is to make a copy (*e.g.*, the record is stored in a computer and a copy must be printed to provide individual access, or the naval activity does not wish to surrender temporarily the original record for the individual to review).

(2) Fee schedules.

(i) Office copy (per page).....$.10

(ii) Microfiche (per fiche).....$.25

(3) Fee waivers. Waive fees automatically if the direct cost of reproduction is less than $15, unless the individual is seeking an obvious extension or duplication of a previous request for which he or she was granted a waiver. Decisions to waive or reduce fees that exceed $15 are made on a case-by-case basis.

(c) *Denying individual access.* (1) Deny the record subject access to requested record only if it was compiled in reasonable anticipation of a civil action or proceeding or is in a system of records that has been exempt from the access provisions of § 701.113.

(2) Deny the individual access only to those portions of the record for which the denial will serve a legitimate government purpose. An individual may be refused access for failure to comply with established procedural requirements, but must be told the specific reason for the refusal and the proper access procedures.

(3) Deny the individual access to his or her medical and psychological records if it is determined that access could have an adverse affect on the mental or physical health of the individual. This determination normally should be made in consultation with a medical practitioner. If it is medically indicated that access could have an adverse mental or physical effect on the individual, provide the record to a medical practitioner named by the individual, along with an explanation of why access without medical supervision could be harmful to the individual. In any case, do not require the named medical practitioner to request the record for the individual. If, however, the individual refuses or fails to designate a medical practitioner, access shall be refused. The refusal is not considered a denial for reporting purposes under the Privacy Act.

(d) Notifying the individual. Written denial of access must be given to the individual. The denial letter shall include:

(1) The name, title, and signature of a designated denial authority;

(2) The date of the denial;

(3) The specific reason for the denial, citing the appropriate subsections of 5 U.S.C. 552a or this subpart and subpart G of this part authorizing the denial;

(4) The individual's right to appeal the denial within 60 calendar days of the date the notice is mailed; and

(5) The title and address of the review authority.

§ 701.110 Amendment of records.

(a) *Individual review and amendment.* Encourage individuals to review periodically, the information maintained about them in systems of records, and to avail themselves of the amendment procedures established by this subpart and subpart G of this part.

(1) *Right to amend.* An individual may request to amend any record retrieved by his or her personal identifier from a system of records, unless the system

has been exempt from the amendment procedures under this subpart. Amendments under this subpart and subpart G of this part are limited to correcting factual matters, not matters of opinion (*i.e.*, information contained in evaluations of promotion potential or performance appraisals). When records sought to be amended are covered by another issuance, the administrative procedures under that issuance must be exhausted before using the Privacy Act. In other words, the Privacy Act may not be used to avoid the administrative procedures required by the issuance actually covering the records in question.

(2) *In writing.* Amendment requests shall be in writing, except for routine administrative changes, such as change of address.

(3) *Content of amendment request.* An amendment request must include a description of the information to be amended; the reason for the amendment; the type of amendment action sought (*i.e.*, deletion, correction, or addition); and copies of available documentary evidence supporting the request.

(b) *Burden of proof.* The individual must provide adequate support for the request.

(c) *Verifying identity.* The individual may be required to provide identification to prevent the inadvertent or intentional amendment of another's record. Use the verification guidelines provided in § 701.109(a)(4).

(d) *Limits on amending judicial and quasi-judicial evidence and findings.* This subpart and subpart G of this part do not permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Amendments to such records must be made in accordance with procedures established for such proceedings. This subpart and subpart G of this part do not permit a collateral attack on a judicial or quasi-judicial finding; however, this subpart and subpart G of this part may be used to challenge the accuracy of recording the finding in a system of records.

(e) *Standards for amendment request determinations.* The record which the individual requests to be amended must meet the recordkeeping standards established in § 701.105. The record must be accurate, relevant, timely, complete, and necessary. If the record in its present state does not meet each of the criteria, grant the amendment request to the extent necessary to meet them.

(f) *Time limits.* Within 10 working days of receiving an amendment request, the systems manager shall provide the individual a written acknowledgement of the request. If action on the amendment request is completed within the 10 working days and the individual is so informed, no separate acknowledgment is necessary. The acknowledgment must clearly identify the request and advise the individual when to expect notification of the completed action. Only under exceptional circumstances should more than 30 working days be required to complete the action on an amendment request.

(g) *Granting an amendment request in whole or in part*—(1) *Notify the requester.* To the extent the amendment request is granted, the systems manager shall notify the individual and make the appropriate amendment.

(2) *Notify previous recipients.* Notify all previous recipients of the information (as reflected in the disclosure accounting record) that the amendment has been made and provide each a copy of the amended record. Recipients who are known to be no longer retaining the record need not be advised of the amendment. If it is known that other naval activities, DoD components, or Federal agencies have been provided the information that now requires amendment, or if the individual requests that these agencies be notified, provide the notification of amendment even if those activities or agencies are not listed on the disclosure accounting form.

(h) *Denying an amendment request in whole or in part.* If the amendment request is denied in whole or in part, promptly notify the individual in writing. Include in the notification to the individual the following:

(1) Those sections of 5 U.S.C. 552a or this subpart and subpart G of this part upon which the denial is based;

(2) His or her right to appeal to the head of the activity for an independent review of the initial denial;

(3) The procedures for requesting an appeal, including the title and address of the official to whom the appeal should be sent; and

(4) Where the individual can receive assistance in filing the appeal.

(i) *Requests for amending OPM records.* The records in an OPM government-wide system of records are only temporarily in the custody of naval activities. Requests for amendment of these records must be processed in accordance with OPM Regulations and the Federal Personnel Manual. The denial authority may deny a request, but all denials are subject to review by the Assistant Director for Workforce Information, Personnel Systems Oversight Group, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415.

(j) *Individual's statement of disagreement.* (1) If the review authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement listing the reasons for disagreeing with the refusal to amend.

(2) If possible, incorporate the statement of disagreement into the record. If that is not possible, annotate the record to reflect that the statement was filed and maintain the statement so that it can be readily obtained when the disputed information is used or disclosed.

(3) Furnish copies of the statement of disagreement to all individuals listed on the disclosure accounting form (except those known to be no longer retaining the record), as well as to all other known holders of copies of the record.

(4) Whenever the disputed information is disclosed for any purpose, ensure that the statement of disagreement also is used or disclosed.

(k) *Department of the Navy statement of reasons.* (1) If the individual files a statement of disagreement, the naval activity may file a statement of reasons containing a concise summary of the activity's reasons for denying the amendment request.

(2) The statement of reasons shall contain only those reasons given to the individual by the appellate official and shall not contain any comments on the individual's statement of disagreement.

(3) At the discretion of the naval activity, the statement of reasons may be disclosed to those individuals, activities, and agencies that receive the statement of disagreement.

§ 701.111 Privacy Act appeals.

(a) *How to file an appeal.* The following guidelines shall be followed by individuals wishing to appeal a denial of notification, access, or amendment of records.

(1) The appeal must be received by the cognizant review authority (*i.e.*, ASN (MRA), NJAG, OGC, or OPM) within 60 calendar days of the date of the response.

(2) The appeal must be in writing and requesters should provide a copy of the denial letter and a statement of their reasons for seeking review.

(b) *Time of receipt.* The time limits for responding to an appeal commence when the appeal reaches the office of the review authority having jurisdiction over the record. Misdirected appeals should be referred expeditiously to the proper review authority.

(c) *Review authorities.* ASN (MRA), NJAG, and OGC are authorized to adjudicate appeals made to SECNAV. NJAG and OGC are further authorized to delegate this authority to a designated Assistant NJAG and the Principal Deputy General or Deputy General Counsel, respectively, under such terms and conditions as they deem appropriate.

(1) If the record is from a civilian Official Personnel Folder or is contained on any other OPM forms, send the appeal to the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415. Records in all systems of records maintained in accordance with the OPM government-wide systems notices are only in the temporary custody of the Department of the Navy.

(2) If the record pertains to the employment of a present or former Navy and Marine Corps civilian employee, such as Navy or Marine Corps civilian personnel records or an employee's grievance or appeal file, to the General Counsel, Navy Department, 720 Kennon

Street, SE, Washington Navy Yard, Building 36, Washington, DC 20374–5012.

(3) If the record pertains to a present or former military member's fitness reports or performance evaluations to the Assistant Secretary of the Navy (Manpower and Reserve Affairs), Navy Department, Washington, DC 20350–1000.

(4) All other records dealing with present or former military members to the Judge Advocate General, Navy Department, 1322 Patterson Avenue, SE, Suite 3000, Washington Navy Yard, Washington, DC 20374–5066.

(d) *Appeal procedures.* (1) If the appeal is granted, the review authority shall advise the individual that his or her appeal has been granted and provide access to the record being sought.

(2) If the appeal is denied totally or in part, the appellate authority shall advise the reason(s) for denying the appeal, citing the appropriate subsections of 5 U.S.C. 552a or this subpart and subpart G of this part that apply; the date of the appeal determination; the name, title, and signature of the appellate authority; and a statement informing the requester of his or her right to seek judicial relief in the Federal District Court.

(e) *Final action, time limits and documentation.* (1) The written appeal notification granting or denying access is the final naval activity action on the initial request for access.

(2) All appeals shall be processed within 30 working days of receipt, unless the appellate authority finds that an adequate review cannot be completed within that period. If additional time is needed, notify the applicant in writing, explaining the reason for the delay and when the appeal will be completed.

(f) *Denial of appeal by activity's failure to act.* An individual may consider his or her appeal denied if the appellate authority fails to:

(1) Take final action on the appeal within 30 working days of receipt when no extension of time notice was given; or

(2) Take final action within the period established by the notice to the appellate authority of the need for an extension of time to complete action on the appeal.

§ 701.112 Disclosure of records.

(a) *Conditions of disclosure.* (1) 5 U.S.C. 552a prohibits an agency from disclosing any record contained in a system of records to any person or agency, except when the record subject gives written consent for the disclosure or when one of the 12 conditions listed below in this subsection applies.

(2) Except for disclosures made under 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act of 1986 and Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program,'' before disclosing any record from a system of records to any recipient other than a Federal agency, make reasonable efforts to ensure the record is accurate, relevant, timely, and complete for Department of the Navy purposes. Records discovered to have been improperly filed in the system of records should be removed before disclosure.

(i) If validation cannot be obtained from the record itself, the naval activity may contact the record subject (if reasonably available) to verify the accuracy, timeliness, completeness, and relevancy of the information.

(ii) If validation cannot be obtained from the record and the record subject is not reasonably available, advise the recipient that the information is believed to be valid as of a specific date and reveal any factors bearing on the validity of the information.

(b) *Nonconsensual disclosures.* 5 U.S.C. 552a provides 12 instances when a record in a system of records may be disclosed without the written consent of the record subject:

(1) *Disclosures within the Department of Defense.* For purposes of disclosing records, the Department of Defense is considered a single agency; hence, a record may be disclosed to any officer or employee in the Department of Defense (including private contractor personnel who are engaged to perform services needed in connection with the operation of a system of records for a DoD component), who have a need for the record in the performance of their duties, provided this use is compatible with the purpose for which the record is maintained. This provision is based on the ''need to know'' concept.

(i) For example, this may include disclosure to personnel managers, review boards, discipline officers, courts-martial personnel, medical officers, investigating officers, and representatives of the Judge Advocate General, Auditor General, Naval Inspector General, or the Naval Investigative Service, who require the information in order to discharge their official duties. Examples of personnel outside the Department of the Navy who may be included are: Personnel of the Joint Staff, Armed Forces Entrance and Examining Stations, Defense Investigative Service, or the other military departments, who require the information in order to discharge an official duty.

(ii) It may also include the transfer of records between naval components and non-DoD agencies in connection with the Personnel Exchange Program (PEP) and interagency support agreements. Disclosure accountings are not required for intra-agency disclosure and disclosures made in connection with interagency support agreements or the PEP. Although some disclosures authorized by this paragraph might also meet the criteria for disclosure under other exceptions specified in the following paragraphs of this section, they should be treated under this paragraph for disclosure accounting purposes.

(2) *Disclosures required by the FOIA.* (i) A record must be disclosed if required by 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act of 1986, which is implemented by Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program.''

(ii) 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act of 1986 and Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program'' require that records be made available to any person requesting them in writing, unless the record is exempt from disclosure under one of the nine FOIA exemptions. Therefore, if a record is not exempt from disclosure, it must be provided to the requester.

(iii) Certain records, such as personnel, medical, and similar files, are exempt from disclosure under exemption (b)(6) of 5 U.S.C. 552 (1988) as amended by the Freedom of Information Act Reform Act of 1986. Under that exemption, disclosure of information pertaining to an individual can be denied only when the disclosure would be a clearly unwarranted invasion of personal privacy. The first step is to determine whether a viable personal privacy interest exists in these records involving an identifiable living person. The second step is to consider how disclosure would benefit the general public in light of the content and context of the information in question. The third step is to determine whether the identified public interests qualify for consideration. The fourth step is to balance the personal privacy interests against the qualifying public interest. Numerous factors must be considered such as: The nature of the information to be disclosed (*i.e.*, Do individuals normally have an expectation of privacy in the type of information to be disclosed?); importance of the public interest served by the disclosure and probability of further disclosure which may result in an unwarranted invasion of privacy; relationship of the requester to the public interest being served; newsworthiness of the individual to whom the information pertains (*i.e.*, high ranking officer, public figure); degree of sensitivity of the information from the standpoint of the individual or the individual's family, and its potential for being misused to the harm, embarrassment, or inconvenience of the individual or the individual's family; the passage of time since the event which is the topic of the record (*i.e.*, to disclose that an individual has been arrested and is being held for trial by court-martial is normally permitted, while to disclose an arrest which did not result in conviction might not be permitted after the passage of time); and the degree to which the information is already in the public domain or is already known by the particular requester.

(iv) Records or information from investigatory records, including personnel security investigatory records, are exempt from disclosure under the broader standard of ''an unwarranted invasion of personal privacy'' found in exemption (b)(7)(C) of 5 U.S.C. 552. This

broader standard applies only to records or information compiled for law enforcement purposes.

(v) A disclosure under 5 U.S.C. 552 about military members must be in accordance with Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program'', but the following information normally may be disclosed from military personnel records (except for those personnel assigned to sensitive or routinely deployable units, or located in a foreign territory), without a clearly unwarranted invasion of personal privacy: Full name, rank, date of rank, base pay, past duty stations, present duty station and future duty station (if finalized), unless the stations have been determined by the Department of the Navy to be sensitive, routinely deployable, or located in a foreign territory, office or duty telephone number, source of commission, promotion sequence number, awards and decorations, attendance at professional military schools, and duty status at any given time.

(vi) The following information normally may be disclosed from civilian employee records about CONUS employees: Full name, present and past position titles and occupational series, present and past grades, present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious and Distinguished Executive Ranks, and allowances and differentials), past duty stations, present duty station and future duty station (if finalized), including room numbers, shop designations, or other identifying information regarding buildings or places of employment, unless the duty stations have been determined by the Department of the Navy to be sensitive, routinely deployable, or located in a foreign territory, position descriptions, identification of job elements, and those performance standards (but not actual performance appraisals) that the disclosure of which would not interfere with law enforcement programs or severely inhibit Department of the Navy effectiveness.

(viii) Disclosure of home addresses and home telephone numbers normally is considered a clearly unwarranted invasion of personal privacy and is prohibited. However, they may be disclosed if the individual has consented to the disclosure; the disclosure is required by the FOIA; the disclosure is required by another law, such as 42 U.S.C. 653, which provides assistance to states in locating parents who have defaulted on child support payments, or the collection of alimony, and to state and local tax authorities for the purpose of enforcing tax laws. However, care must be taken prior to release to ensure that a written record is prepared to document the reasons for the release determination.

(A) When compiling home addresses and telephone numbers, the individual may be offered the option of authorizing disclosure of the information without further consent for specific purposes, such as locator services. In that case, the information may be disclosed for the stated purpose without further consent. If the information is to be disclosed for any other purpose, a signed consent permitting the additional disclosure must be obtained from the individual.

(B) Before listing home addresses and telephone numbers in Department of the Navy telephone directories, give the individual the opportunity to refuse such a listing. If the individual requests that the home address or telephone number not be listed in the directory, do not assess any additional fee associated with maintaining an unlisted number for government-owned telephone services.

(C) The sale or rental of lists of names and addresses is prohibited unless such action is specifically authorized by Federal law. This does not prohibit the disclosure of names and addresses made under Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program.''

(D) In response to FOIA requests, information concerning special and general courts-martial results (*e.g.*, records of trial) are releasable. However, information regarding summary courts-martial and non-judicial punishment are generally not releasable. The balancing of interests must be done. It

is possible that in a particular case, information regarding non-judicial punishment should be disclosed pursuant to a FOIA request (*i.e.*, the facts leading to a nonjudicial punishment are particularly newsworthy or the case involves a senior official abusing the public trust through office-related misconduct, such as embezzlement). Announcement of nonjudicial punishment dispositions under JAGMAN, subsection 0107, is a proper exercise of command authority and not a release of information under FOIA or this subpart and subpart G of this part. Exceptions to this policy must be coordinated with CNO (N09B30) or CMC (ARAD) prior to responding to requesters, including all requests for this type of information from members of Congress.

(3) *Disclosures for established routine uses.* (i) Records may be disclosed outside the Department of the Navy if the disclosure is for an established routine use.

(ii) A routine use shall:

(A) Be compatible with and related to the purpose for which the record was created;

(B) Identify the persons or organizations to whom the record may be disclosed;

(C) Identify specifically the uses for which the information may be employed by the receiving person or organization; and

(D) Have been published previously in the FEDERAL REGISTER.

(iii) A routine use shall be established for each user of the information outside the Department of the Navy who needs the information for an official purpose.

(iv) Routine uses may be established, discontinued, or amended without the consent of the individuals to whom the records pertain. However, new and amended routine uses must be published in the FEDERAL REGISTER at least 30 days before the information may be disclosed under their provisions.

(v) In addition to the routine uses established by the Department of the Navy for each system of records, common ''Blanket Routine Uses,'' applicable to all record systems maintained with the Department of the Navy, have been established. These ''Blanket Routine Uses'' are published at the beginning of the Department of the Navy's FEDERAL REGISTER compilation of record systems notices rather than at each system notice and are also reflected in periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances.'' Unless a system notice specifically excludes a system of records from a ''Blanket Routine Use,'' all ''Blanket Routine Uses'' apply to that system.

(vi) If the recipient has not been identified in the FEDERAL REGISTER or if the recipient, though identified, intends to employ the information for a purpose not published in the FEDERAL REGISTER, the written consent of the individual is required before the disclosure can be made.

(4) *Disclosures to the Bureau of the Census.* Records may be disclosed to the Bureau of the Census for purposes of planning or carrying out a census, survey, or related activities authorized by 13 U.S.C. 8.

(5) *Disclosures for statistical research or reporting.* Records may be disclosed to a recipient for statistical research or reporting if:

(i) Prior to the disclosure, the recipient has provided adequate written assurance that the records shall be used solely for statistical research or reporting; and

(ii) The records are transferred in a form that does not identify individuals.

(6) *Disclosures to the National Archives and Records Administration.* (i) Records may be disclosed to the National Archives and Records Administration for evaluation to determine whether the records have sufficient historical or other value to warrant preservation by the Federal government. If preservation is warranted, the records will be retained by the National Archives and Record Administration, which becomes the official owner of the records.

(ii) Records may be disclosed to the National Archives and Records Administration to carry out records management inspections required by Federal law.

(iii) Records transferred to a Federal Records Center operated by the National Archives and Records Administration for storage are not within this

category. Those records continue to be maintained and controlled by the transferring naval activity. The Federal Records Center is considered the agent of Department of the Navy and the disclosure is made under paragraph (b)(1) of this section.

(7) *Disclosures when requested for law enforcement purposes.* (i) A record may be disclosed to another agency or an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity if:

(A) The civil or criminal law enforcement activity is authorized by law (federal, state or local); and

(B) The head of the agency (or his or her designee) has made a written request to the naval activity specifying the particular record or portion desired and the law enforcement purpose for which it is sought.

(ii) Blanket requests for any and all records pertaining to an individual shall not be honored. The requesting agency must specify each record or portion desired and how each relates to the authorized law enforcement activity.

(iii) If a naval activity discloses a record outside the Department of Defense for law enforcement purposes without the individual's consent and without an adequate written request, the disclosure must be under an established routine use, such as the ''Blanket Routine Use'' for law enforcement.

(iv) Disclosure to foreign law enforcement agencies is not governed by the provisions of 5 U.S.C. 552a and this paragraph, but may be made only under established ''Blanket Routine Uses,'' routine uses published in the individual record system notice, or to other governing authority.

(8) *Disclosure to protect the health or safety of an individual.* Disclosure may be made under emergency conditions involving circumstances affecting the health and safety of an individual (*i.e.,* when the time required to obtain the consent of the individual to whom the records pertain might result in a delay which could impair the health or safety of a person) provided notification of the disclosure is sent to the record subject. Sending the notification to the last known address is sufficient. In instances where information is requested by telephone, an attempt will be made to verify the inquirer's and medical facility's identities and the caller's telephone number. The requested information, if then considered appropriate and of an emergency nature, may be provided by return call.

(9) *Disclosures to Congress.* (i) A record may be disclosed to either House of Congress at the request of either the Senate or House of Representatives as a whole.

(ii) A record also may be disclosed to any committee, subcommittee, or joint committee of Congress if the disclosure pertains to a matter within the legislative or investigative jurisdiction of the committee, subcommittee, or joint committee.

(iii) Disclosure may not be made to a Member of Congress requesting in his or her individual capacity. However, for Members of Congress making inquiries on behalf of individuals who are subjects of records, a ''Blanket Routine Use'' has been established to permit disclosures to individual Members of Congress.

(A) When responding to a congressional inquiry made on behalf of a constituent by whose identifier the record is retrieved, there is no need to verify that the individual has authorized the disclosure to the Member of Congress.

(B) The oral or written statement of a Congressional staff member is sufficient to establish that a request has been received from the individual to whom the record pertains.

(C) If the constituent inquiry is made on behalf of an individual other than the record subject, provide the Member of Congress only that information releasable under 5 U.S.C. 552. Advise the Member of Congress that the written consent of the record subject is required before additional information may be disclosed. Do not contact the record subject to obtain consent for the disclosure to the Member of Congress unless the Congressional office specifically requests it be done.

(10) *Disclosures to the Comptroller General for the General Accounting Office (GAO).* Records may be disclosed to the Comptroller General of the U.S., or authorized representative, in the course

of the performance of the duties of the GAO.

(11) *Disclosures under court orders.* (i) Records may be disclosed under the order of a court of competent jurisdiction.

(ii) When a record is disclosed under this provision and the compulsory legal process becomes a matter of public record, make reasonable efforts to notify the individual to whom the record pertains. Notification sent to the last known address of the individual is sufficient. If the order has not yet become a matter of public record, seek to be advised as to when it will become public. Neither the identity or the party to whom the disclosure was made nor the purpose of the disclosure shall be made available to the record subject unless the court order has become a matter of public record.

(iii) The court order must bear the signature of a federal, state, or local judge. Orders signed by court clerks or attorneys are not deemed to be orders of a court of competent jurisdiction. A photocopy of the order, regular on its face, will be sufficient evidence of the court's exercise of its authority of the minimal requirements of SECNAVINST 5820.8A,[9] ''Release of Official Information for Litigation Purposes and Testimony by Department of the Navy Personnel.''

(12) *Disclosures to consumer reporting agencies.* Certain information may be disclosed to consumer reporting agencies (i.e., credit reference companies such as TRW and Equifax, etc.) as defined by the Federal Claims Collection Act of 1966 (31 U.S.C. 952d). Under the provisions of that Act, the following information may be disclosed to a consumer reporting agency:

(i) Name, address, taxpayer identification number (SSN), and other information necessary to establish the identity of the individual;

(ii) The amount, status, and history of the claim; and

(iii) The agency or program under which the claim arose. 31 U.S.C. 952d specifically requires that the FEDERAL REGISTER notice for the system of records from which the information will be disclosed indicate that the information may be disclosed to a consumer reporting agency.

(c) *Disclosures to commercial enterprises.* Records may be disclosed to commercial enterprises only under the criteria established by Secretary of the Navy Instruction 5720.42F and 42 U.S.C. 653, Parent Locator Service for Enforcement of Child Support.

(1) Any information required to be disclosed by Secretary of the Navy Instruction 5720.42F and 42 U.S.C. 653, Parent Locator Service for Enforcement of Child Support may be disclosed to a requesting commercial enterprise.

(2) Commercial enterprises may present a consent statement signed by the individual indicating specific conditions for disclosing information from a record. Statements such as the following, if signed by the individual, are considered sufficient to authorize the disclosure: I hereby authorize the Department of the Navy to verify my SSN or other identifying information and to disclose my home address and telephone number to authorized representatives of (name of commercial enterprise) to be used in connection with my commercial dealings with that enterprise. All information furnished will be used in connection with my financial relationship with (name of commercial enterprise).

(3) When a consent statement as described in the preceding subsection is presented, provide the information to the commercial enterprise, unless the disclosure is prohibited by another regulation or Federal law.

(4) Blanket consent statements that do not identify the Department of Defense or Department of the Navy, or that do not specify exactly the information to be disclosed, may be honored if it is clear that the individual, in signing the consent statement, was seeking a personal benefit (i.e., loan for a house or automobile) and was aware of the type of information necessary to obtain the benefit sought.

(5) Do not honor requests from commercial enterprises for official evaluations of personal characteristics such as personal financial habits.

[9] Copies may be obtained: Judge Advocate General, Navy Department, (Code 34), 1322 Patterson Avenue, SE, Suite 3000, Washington Navy Yard, Washington, DC 20374–5066.

(d) *Disclosure of health care records to the public.* This paragraph applies to disclosure of information to the news media and the public concerning individuals treated or hospitalized in Department of the Navy medical facilities and, when the cost of care is paid by the Department of the Navy, in non-Federal facilities.

(1) *Disclosures without the individual's consent.* Normally, the following information may be disclosed without the individual's consent:

(i) Information required to be released by Secretary of the Navy Instruction 5720.42F and OPM Regulations and the Federal Personnel Manual, as well as the information listed in paragraphs (b)(2)(v) (for military personnel) and (b)(2) of this section.

(ii) For civilian employees; and

(iii) General information concerning medical conditions, i.e., date of admission or disposition; present medical assessment of the individual's condition if the medical practitioner has volunteered the information, i.e., the individual's condition presently is (stable) (good) (fair) (serious) (critical), and the patient is (conscious) (semi-conscious) (unconscious).

(2) *Disclosures with the individual's consent.* With the individual's informed consent, any information about the individual may be disclosed. If the individual is a minor or has been declared incompetent by a court of competent jurisdiction, the parent of the minor or appointed legal guardian of the incompetent may give consent on behalf of the individual.

(e) Disclosure of Personal Information on Group/Bulk Orders. Do not use personal information including complete SSNs, home addresses and phone numbers, dates of birth, etc., on group/bulk orders. This personal information should not be posted on lists that everyone listed on the orders sees. Such a disclosure of personal information violates the Privacy Act and this subpart and subpart G of this part.

(f) *Disclosure accounting.* Keep an accurate record of all disclosures made from a record (including those made with the consent of the individual) except those made to DoD personnel for use in performing their official duties; and those made under the FOIA. Disclosure accounting is to permit the individual to determine what agencies or persons have been provided information from the record, enable Department of the Navy activities to advise prior recipients of the record of any subsequent amendments or statements of dispute concerning the record, and provide an audit trial of Department of the Navy's compliance with 5 U.S.C. 552a.

(1) Disclosure accountings shall contain the date of the disclosure; a description of the information disclosed; the purpose of the disclosure; and the name and address of the person or agency to whom the disclosure was made.

(2) The record subject has the right of access to the disclosure accounting except when the disclosure was made at the request of a civil or criminal law enforcement agency under paragraph (b)(7) of this section; or when the system of records has been exempted from the requirement to provide access to the disclosure accounting.

(g) *Methods of disclosure accounting.* Since the characteristics of various records maintained within the Department of the Navy vary widely, no uniform method for keeping disclosure accountings is prescribed. The primary criteria are that the selected method be one which will:

(1) Enable an individual to ascertain what persons or agencies have received disclosures pertaining to him/her;

(2) Provide a basis for informing recipients of subsequent amendments or statements of dispute concerning the record; and

(3) Provide a means to prove, if necessary that the activity has complied with the requirements of 5 U.S.C. 552a and this subpart and subpart G of this part.

(h) *Retention of disclosure accounting.* Maintain a disclosure accounting of the life of the record to which the disclosure pertains, or 5 years after the date of the disclosure, whichever is longer. Disclosure accounting records are normally maintained with the record, as this will ensure compliance with paragraph (f) of this section.

§ 701.113 Exemptions.

(a) *Using exemptions.* No system of records is automatically exempt from all provisions of 5 U.S.C. 552a. A system of records is exempt from only those provisions of 5 U.S.C. 552a that are identified specifically in the exemption rule for the system. Subpart G of this part contains the systems designated as exempt, the types of exemptions claimed, the authority and reasons for invoking the exemptions and the provisions of 5 U.S.C. 552a from which each system has been exempt. Exemptions are discretionary on the part of Department of the Navy and are not effective until published as a final rule in the FEDERAL REGISTER. The naval activity maintaining the system of records shall make a determination that the system is one for which an exemption may be established and then propose an exemption rule for the system. Submit the proposal to CNO (N09B30) for approval and publication in the FEDERAL REGISTER.

(b) *Types of exemptions.* There are two types of exemptions permitted by 5 U.S.C. 552a.

(1) *General exemptions.* Those that authorize the exemption of a system of records from all but specifically identified provisions of 5 U.S.C. 552a.

(2) *Specific exemptions.* Those that allow a system of records to be exempt from only a few designated provisions of 5 U.S.C. 552a.

(c) *Establishing exemptions.* (1) 5 U.S.C. 552a authorizes the Secretary of the Navy to adopt rules designating eligible systems of records as exempt from certain requirements. The Secretary of the Navy has delegated the CNO (N09B30) to make a determination that the system is one for which an exemption may be established and then propose and establish an exemption rule for the system. No system of records within Department of the Navy shall be considered exempt until the CNO (N09B30) has approved the exemption and an exemption rule has been published as a final rule in the FEDERAL REGISTER. A system of records is exempt from only those provisions of 5 U.S.C. 552a that are identified specifically in the Department of the Navy exemption rule for the system.

(2) No exemption may be established for a system of records until the system itself has been established by publishing a notice in the FEDERAL REGISTER, at least 30 days prior to the effective date, describing the system. This allows interested persons an opportunity to comment. An exemption may not be used to deny an individual access to information that he or she can obtain under Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program.''

(d) *Exemption for classified material.* All systems of records maintained by the Department of the Navy shall be exempt under section (k)(1) of 5 U.S.C. 552a, to the extent that the systems contains any information properly classified under E.O. 12958 and that is required by that E.O. to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein which contain isolated items of properly classified information.

NOTE: Department of the Navy Privacy Act systems of records which contain classified information automatically qualify for a (k)(1) exemption, without establishing an exemption rule.

(e) *Exempt records in nonexempt systems.* (1) An exemption rule applies to the system of records for which it was established. If a record from an exempt system is incorporated intentionally into a system that has not been exempt, the published notice and rules for the nonexempt system will apply to the record and it will not be exempt from any provisions of 5 U.S.C. 552a.

(2) A record from one component's (i.e., Department of the Navy) exempted system that is temporarily in the possession of another component (i.e., Army) remains subject to the published system notice and rules of the originating component's (i.e., Department of the Navy). However, if the non-originating component incorporates the record into its own system of records, the published notice and rules for the system into which it is incorporated shall apply. If that system of records has not been exempted, the record shall

not be exempt from any provisions of 5 U.S.C. 552a.

(3) A record accidentally misfiled into a system of records is governed by the published notice and rules for the system of records in which it actually should have been filed.

(f) *General exemptions*—(1)*Central Intelligence Agency (CIA).* The Department of the Navy is not authorized to establish an exemption for records maintained by the CIA under subsection (j)(1) of 5 U.S.C. 552a.

(2) *Law enforcement.* (i) The general exemption provided by subsection (j)(2) of 5 U.S.C. 552a may be established to protect criminal law enforcement records maintained by Department of the Navy.

(ii) To be eligible for the (j)(2) exemption, the system of records must be maintained by an element that performs, as one of its principal functions, the enforcement of criminal laws. The Naval Investigative Service, Naval Inspector General, and military police activities qualify for this exemption.

(iii) Criminal law enforcement includes police efforts to detect, prevent, control, or reduce crime, or to apprehend criminals, and the activities of prosecution, court, correctional, probation, pardon, or parole authorities.

(iv) Information that may be protected under the (j)(2) exemption includes:

(A) Information compiled for the purpose of identifying criminal offenders and alleged criminal offenders consisting of only identifying data and notations of arrests; the nature and disposition of criminal charges; and sentencing, confinement, release, parole, and probation status;

(B) Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; and

(C) Reports identifiable to an individual, compiled at any stage of the enforcement process, from arrest, apprehension, indictment, or preferral of charges through final release from the supervision that resulted from the commission of a crime.

(v) The (j)(2) exemption does not apply to:

(A) Investigative records maintained by a naval activity having no criminal law enforcement duties as one of its principle functions, or

(B) Investigative records compiled by any element concerning individual's suitability, eligibility, or qualification for duty, employment, or access to classified information, regardless of the principle functions of the naval activity that compiled them.

(vi) The (j)(2) exemption established for a system of records maintained by a criminal law enforcement activity cannot protect law enforcement records incorporated into a nonexempt system of records or any system of records maintained by an activity not principally tasked with enforcing criminal laws. All system managers, therefore, are cautioned to comply strictly with Department of the Navy regulations or instructions prohibiting or limiting the incorporation of criminal law enforcement records into systems other than those maintained by criminal law enforcement activities.

(g) *Specific exemptions.* Specific exemptions permit certain categories of records to be exempted from specific provisions of 5 U.S.C. 552a. Subsections (k)(1)–(k)(7) of 5 U.S.C. 552a allow exemptions for seven categories of records. To be eligible for a specific exemption, the record must meet the corresponding criteria.

NOTE: Department of the Navy Privacy Act systems of records which contain classified information automatically qualify for a (k)(1) exemption, without an established exemption rule.

(1) *(k)(1) exemption:* Information properly classified under Secretary of the Navy Instruction 5720.42F, ''Department of the Navy Freedom of Information Act Program'' and E.O. 12958, in the interest of national defense or foreign policy.

(2) *(k)(2) exemption:* Investigatory information (other than that information within the scope of paragraph (f)(2) of this section) compiled for law enforcement purposes. If maintaining the information causes an individual to be ineligible for or denied any right, benefit, or privilege that he or she would otherwise be eligible for or entitled to under Federal law, then he or she shall be given access to the information, except for the information that would

identify a confidential source (see paragraph (h) of this section, ''confidential source''). The (k)(2) exemption, when established, allows limited protection on investigative records maintained for use in personnel and administrative actions.

(3) *(k)(3) exemption:* Records maintained in connection with providing protective services to the President of the United States and other individuals under 18 U.S.C. 3056.

(4) *(k)(4) exemption:* Records required by Federal law to be maintained and used solely as statistical records that are not used to make any determination about an identifiable individual, except as provided by 13 U.S.C. 8.

(5) *(k)(5) exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source (see paragraph (h) of this section, ''confidential source''). This exemption allows protection of confidential sources in background investigations, employment inquiries, and similar inquiries used in personnel screening to determine suitability, eligibility, or qualifications.

(6) *(k)(6) exemption:* Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal or military service if the disclosure would compromise the objectivity or fairness of the testing or examination process.

(7) *(k)(7) exemption:* Evaluation material used to determine potential for promotion in the military services, but only to the extent that disclosure would reveal the identity of a confidential source (see paragraph (h) of this section, ''confidential source''.)

(h) *Confidential source.* Promises of confidentiality are to be given on a limited basis and only when essential to obtain the information sought. Establish appropriate procedures for granting confidentiality and designate those categories of individuals authorized to make such promises.

§ 701.114 Enforcement actions.

(a) *Administrative remedies.* An individual who alleges he or she has been affected adversely by a naval activity's violation of 5 U.S.C. 552a or this subpart and subpart G of this part shall be permitted to seek relief from SECNAV through proper administrative channels.

(b) *Civil court actions.* After exhausting all administrative remedies, an individual may file suit in Federal court against a naval activity for any of the following acts:

(1) *Denial of an amendment request.* The activity head, or his or her designee wrongfully refuses the individual's request for review of the initial denial of an amendment or, after review, wrongfully refuses to amend the record;

(2) *Denial of access.* The activity wrongfully refuses to allow the individual to review the record or wrongfully denies his or her request for a copy of the record;

(3) *Failure to meet recordkeeping standards.* The activity fails to maintain an individual's record with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination about the individual's rights, benefits, or privileges and, in fact, makes an adverse determination based on the record; or

(4) *Failure to comply with Privacy Act.* The activity fails to comply with any other provision of 5 U.S.C. 552a or any rule or regulation promulgated under 5 U.S.C. 552a and thereby causes the individual to be adversely affected.

(c) *Criminal penalties.* Subsection (i)(1) of 5 U.S.C. 552a authorizes three criminal penalties against individuals for violations of its provisions. All three are misdemeanors punishable by fines of $5,000.

(1) *Wrongful disclosure.* Any member or employee of Department of the Navy who, by virtue of his or her employment or position, has possession of or access to records and willfully makes a disclosure knowing that disclosure is in violation of 5 U.S.C. 552a or this subpart and subpart G of this part.

(2) *Maintaining unauthorized records.* Any member or employee of Department of the Navy who willfully maintains a system of records for which a

notice has not been published under periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances.''

(3) *Wrongful requesting or obtaining records.* Any person who knowingly and willfully requests or obtains information concerning an individual under false pretenses.

§ 701.115 Computer matching program.

(a) *General.* 5 U.S.C. 552a and this subpart and subpart G of this part are applicable to certain types of computer matching, i.e., the computer comparison of automated systems of records. There are two specific kinds of matching programs that are fully governed by 5 U.S.C. 552a and this subpart and subpart G of this part:

(1) Matches using records from Federal personnel or payroll systems of records;

(2) Matches involving Federal benefit programs to accomplish one or more of the following purposes:

(i) To determine eligibility for a Federal benefit.

(ii) To comply with benefit program requirements.

(iii) To effect recovery of improper payments or delinquent debts from current or former beneficiaries.

(b) *The record comparison must be a computerized one.* Manual comparisons are not covered, involving records from two or more automated systems of records (i.e., systems of records maintained by Federal agencies that are subject to 5 U.S.C. 552a); or a Department of the Navy automated systems of records and automated records maintained by a non-Federal agency (i.e., State or local government or agent thereof). A covered computer matching program entails not only the actual computerized comparison, but also preparing and executing a written agreement between the participants, securing approval of the Defense Data Integrity Board, publishing a matching notice in the FEDERAL REGISTER before the match begins, ensuring that investigation and due process are completed, and taking ultimate action, if any.

Subpart G—Privacy Act Exemptions

AUTHORITY: Pub. L. 93–579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 65 FR 31471, May 18, 2000, unless otherwise noted.

§ 701.116 Purpose.

Subparts F and G of this part contain rules promulgated by the Secretary of the Navy, pursuant to 5 U.S.C. 552a (j) and (k), and subpart F, § 701.113, to exempt certain systems of Department of the Navy records from specified provisions of 5 U.S.C. 552a.

§ 701.117 Exemption for classified records.

All systems of records maintained by the Department of the Navy shall be exempt from the requirements of the access provision of the Privacy Act (5 U.S.C. 552a(d)) under the (k)(1) exemption, to the extent that the system contains information properly classified under E.O. 12958 and that is required by that E.O. to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein which contain isolated items of properly classified information.

§ 701.118 Exemptions for specific Navy record systems.

(a) *System identifier and name:*

(1) *N01070–9, White House Support Program.*

(2) *Exemption:* (i) Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure